BSTZ No. 42390P11398
Express Mail No. EL105935949US

UNITED STATES PATENT APPLICATION

FOR

CONNECTIVITY TO PUBLIC DOMAIN SERVICES OF WIRELESS LOCAL AREA NETWORKS

Inventors

Jiewen Liu
Shahrnaz Azizi

Prepared by:

Blakely, Sokoloff, Taylor & Zafman LLP
12400 Wilshire Boulevard, Suite 700
Los Angeles, California 90025
(714) 557-3800

CONNECTIVITY TO PUBLIC DOMAIN SERVICES OF WIRELESS LOCAL AREA NETWORKS

Field

The invention relates to wireless local area networks. In particular, one embodiment of the invention relates to a method, machine-readable medium, and apparatus for providing simple access to public computer network services to non-authorized wireless local area network users.

Background

Wireless local area networks (WLAN) have developed to provide communication capabilities to various types of mobile devices. Such communication capabilities enable mobile devices to communicate with other devices in the network and beyond.

A typical WLAN has an interface point or access point (AP) to enable communications to, from, and/or between wireless devices within its network. An AP is the point of entry for wireless devices or mobile units (MU) into a network infrastructure. Additionally, an AP may itself be communicatively coupled to other network(s) including a wired network. Thus, an AP may manage communications between itself and other devices within its wireless network, communications between devices within its wireless network, and act as a bridge or gateway for communications between devices within its network and devices outside of its networks (e.g., devices on a wired network).

One type of WLAN has been specified in the Institute of Electrical and Electronics Engineers (IEEE) Standard 802.11 - 1997 and subsequent revisions. In an IEEE 802.11 compliant wireless network, various services are provided to establish and manage communications between an AP and MUs. Generally, an MU is registered, pre-subscribed, or otherwise authorized to access and/or communicate over the WLAN through the AP.

For example, a WLAN may be deployed within a corporation. The corporation wishes to protect its computers and data that can be accessed over the network. Thus, an AP may limit access to the network to only pre-authorized MUs. A first mobile unit, being a pre-authorized device, would be allowed to communicate over the network. Meanwhile, a second mobile unit would be denied access to the network since it is not a pre-authorized device.

A typical network access protocol for an IEEE 802.11 compliant WLAN is herein described. Upon start-up or initialization, an MU with an IEEE 802.11 compliant interface attempts to find an existing WLAN infrastructure. The MU may listen to the information broadcasted by a WLAN station or AP. This information would allow the MU to locate AP, and then possibly to join its network. The MU may also start by sending out a message to solicit such information from a WLAN station or AP. The MU may then listen for a response from AP. The AP receiving such a request responds by sending a message with information that will allow the MU to locate the WLAN infrastructure. Once the MU has found an infrastructure, it may choose to join the WLAN by synchronizing its parameters.

If the MU decides to join a WLAN, it then proceeds by authentication/association handshakes. The authentication process is a mechanism for the MU to prove it's identity . The IEEE 802.11 1997 WLAN specification supports two authentication services, Open System and Shared Key. These services function as low-level interfaces to negotiate access to the WLAN. Recent extensions of the IEEE 802.11 supports more enhanced authentication methods to improve security. Open System authentication is a default, null authentication procedure or algorithm. This procedure involves identity assertion, request for authentication, and an authentication result. Typically, an MU is already a network member, provides a password, and/or is pre-registered, in order to obtain access to the WLAN and its services via the

authentication interface. Other authentication algorithms typically require MUs to know a secret key. The secret key may be delivered to an MU over a secure channel that may be protocol independent of the IEEE 802.11 standard (e.g., the IEEE 802.1x standard for instance).

Association is the mechanism through which an IEEE 802.11 compliant WLAN provides transparent mobility to stations or APs. Once a station successfully completes authentication/association handshakes with an AP, it may begin exchanging data frames with the AP and accessing network services.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 illustrates one method of implementing public mode access according to one embodiment of the invention.

Figure 2 illustrates an exemplary menu of various pay and free public domain services that may be provided to a mobile unit.

Figure 3 illustrates one embodiment of the invention that provides multiple access modes through multiple access points to permit both authorized and non-authorized mobile units to access network services.

Figure 4 illustrates another embodiment of the invention that provides multiple access modes through a single access point to permit both authorized and non-authorized mobile units to access network services.

Figure 5 illustrates a block diagram of one embodiment of an access point device according to one aspect of the invention.

DETAILED DESCRIPTION OF THE INVENTION

In the following detailed description of the invention, numerous specific details are set forth in order to provide a thorough understanding of the invention. However, the invention may be practiced without these specific details. In other instances well known methods, procedures, and/or components have not been described in detail so as not to unnecessarily obscure aspects of the invention.

Throughout this description, the term 'mobile unit' (MU) generally refers to any device with a wireless communication interface that may be used to access a WLAN. Additionally, the term 'authorization' generally refers to any pre-subscription or authentication scheme whereby a prior registration, password, and/or relationship is established to permit an MU to gain access to a network. Conversely, the term 'non-authorized' generally refers to MU or users that have no prior registration, agreement, and/or authority to access a network. The term 'public domain' generally refers to both free and/or pay-per-use network services that made available to non-authorized MUs and/or users. The term 'network services' generally refers to access to various data, information, applications, and/or communication interfaces provided by a network. In the context in which it is employed herein, network services may refer to services provided by a wireless and/or wired network.

One aspect of the invention provides a novel scheme that permits non-authorized MUs to access public or limited regions of a network. In one implementation, this enables an IEEE 802.11 compliant WLAN to provide access to services of its own network (e.g. a wireless network) and/or of other networks (e.g. a wired network) to non-authorized wireless devices.

Generally, conventional WLANs implementations restrict access to network services (e.g. wireless network services and/or wired network services) to authorized users or MUs.

This may be accomplished in a number of ways. In one implementation access to the WLAN is restricted to authorized MUs only by requiring secret key access during authentication. In other implementations, a higher-level access restriction scheme may be employed. This higher-level access restriction scheme may necessitate that the MU continuously provide some security identification, authentication password or key, or that the MU be known (or pre-registered) to the AP network beforehand.

One aspect of the invention provides multiple access modes through an AP to permit both authorized and non-authorized MUs to access network services. According to one implementation, an AP has two modes of operation, private mode and public mode.

In private mode, the AP and MU first implement Secure Service, as specified in the IEEE 802.11 (or its supplements) specification, including authentication and encryption to ensure secure communications over the WLAN. Then, the AP provides full network access/ functionality to the MU consistent with the IEEE 802.11 Standard WLAN specification.

In public mode, an AP provides non-authorized MUs access to public network services. Establishing a connection between an MU and AP in public mode differs from how a connection is established in private mode.

Generally, connection establishment between an AP and MU refers to completing authentication and association handshakes regardless of their order. For instance, in one embodiment authentication may be performed prior to association, while in another embodiment authentication may be performed after association.

An AP operating in public mode may provide non-authorized MUs access to network services by first initiating a simple registration process.

According to one aspect of the invention, the Open System and/or other authentication procedures are supplemented to

provide non-authorized MUs free and/or pay-per-use access to certain WLAN services. The network services available to non-authorized MUs are provided to the user for selection. In this manner, non-authorized MUs may access a number of network services while restricting access to private network services (such as those belonging to a corporation) to authorized MUs only.

Figure 1 illustrates one method of implementing public mode access according to one embodiment of the invention. An AP may be pre-configured or dynamically configured to operate in public mode 102. This may occur at start-up or boot-up for example. An MU then sends a request to obtain basic connection information (or the MU awaits for such information) 104. The AP responds to the request by indicating its mode of operation (either public mode or private mode) 106.

In one implementation, the AP operating in public mode responds by indicating public mode operation and providing the available WLAN service information 106. The WLAN services available in public mode may also be referred to as public domain services.

In public mode, the MU and AP may then process authentication information 108 to establish an initial connection with the AP.

Once the initial connection has been established, the MU displays the WLAN public domain services available and waits for user selection 110. Figure 2 illustrates an exemplary menu of various pay and free public domain services that may be displayed on an MU.

If the public domain services are freely accessible, once the user selects a service the, network connection will be established and normal operation of the selected service(s) may begin 122. An AP terminates access to network services by sending a disconnect notice 126. In this manner, a non-authorized MU may obtain access to public domain services of a

network, while allowing other network services to be secure from unauthorized access.

If the user selects a pay-for-use public domain service, then some form of payment will be requested. In one implementation, secure services are provided to safeguard the transaction 112. Different forms of payment options may be displayed by the MU to enable a user to provide payment 114. The AP and MU employ a secure scheme 112 to prevent easy access to payment information (e.g. credit card number, etc.) during transmission from the MU to the AP. In various embodiments, a user may provide payment via credit card, prepaid services (e.g. prepaid phone-card), and/or other forms of remote or direct payment methods.

Once an AP receives payment information 116 (e.g. credit card number), it passes this information to other network components for validation 118 in a secure way. Validation is the process of checking the validity of the form of payment sent by the MU to the AP as payment for a pay for use service. The AP is informed of the validation results. The AP, in turn, sends the result to the MU 120.

If the form of payment is determined to be valid, the connection of the MU to the selected service 124 through an AP 122 is established.

If a prepaid payment form is used, a timer is maintained to monitor the amount of time the service is employed. If the prepaid time is exceeded, then service is terminated. In one implementation, the MU maintains a timer to indicate the amount of prepaid time used or remaining. In another implementation, a timer is maintained by the AP, enabling the AP to terminate access to network services if the prepaid time has been exhausted. In other implementations, the AP may terminate access to public domain network services if such access has exceeded an allotted amount of time and/or if network traffic reaches a threshold level (e.g. to alleviate network congestion).

Figure 3 illustrates one embodiment of the invention that provides multiple access modes through multiple access points to permit both authorized and non-authorized MUs to access network services. A first access point AP1 302 is communicatively coupled to a network and configured to operate in private mode and provide network services (e.g. pre-registered) to authorized MUs (e.g. MU1 306). A second access point AP2 304 is communicatively coupled to the same network and configured to operate in public mode and provide public domain service(s) (e.g. free or pay-per-use) to non-authorized MUs (e.g. MU2 308).

Figure 4 illustrates another embodiment of the invention that provides multiple access modes through a single access point to permit both authorized and non-authorized MUs to access network services. An access point AP 402 is communicatively coupled to a network and configured to provide both private mode network service(s) (e.g. pre-registered) to authorized MUs (e.g. MU1 406) and public mode service(s) (e.g. free or pay-per-use) to non-authorized MUs (e.g. MU2 408). In one embodiment, AP 402 may have a single wireless communication port (e.g. a wireless transceiver port) concurrently supporting both public and private mode communications and/or services. In another embodiment, AP 402 may have two separate wireless communications ports (e.g. wireless transceiver ports), a first port to support public mode communications and/or services and a second port to support private mode communications and/or services.

Figure 5 illustrates one embodiment of an access point AP device 500 according to one aspect of the invention. A transceiver port 502 serves to wirelessly transmit and receive information from mobile devices and/or users. The wireless transceiver port 502 is coupled to a control unit 504 that controls communications/access between the transceiver port 502 and a network communications port 506 (unit 504 is also handles 802.11 protocol). The network communications port 506

to couple to a wired or wireless network. Through both the transceiver port 502 and network communications point 506, the access point device 500 acts as a gateway for wireless/mobile devices to access network services.

In a first mode of operation (e.g. private mode), the access point device 500 permits authorized mobile devices access to the network communications port 506 and the network services provided by the network coupled to the network communications port 506. In this mode of operation, only mobile devices that are pre-authorized or are members of the network may obtain access to network services via the network communications port 506.

In a second mode of operation (e.g. public mode), the access point device 500 permits non-authorized mobile devices access to the network communications port 506 and the public domain network services provided by the network coupled to the network communications port 506.

The access point device is configured to provide non-member or non-authorized MUs a list of available public domain (e.g. free or pay-per-use) network services. The MU user may select from the list of public domain services and thus obtain access to the selected services. If a pay-per-use network service is selected, then the access point device 500 provides a mechanism to validate such payment information prior to permitting the MU access to the selected network service. The access point device 500 may request that the MU user provide a form of payment (e.g. credit card number, prepaid card, etc.). Upon receiving said payment information, the access point device 500 validates the form of payment to ascertain that it is bona fide. The access point device 500 may employ network services, over the network communications port 506, to validate the payment information.

The access point device 500 communicates with MUs in accordance with the Electrical and Electronics Engineers (IEEE) Standard 802.11 Specification. In particular,

authentication and privacy services may be provided via the procedures defined in IEEE Standard 802.11 and/ or any of its supplement Specifications.

In another embodiment, the access point device 500 may operate to provide both authorized and non-authorized MU (e.g. members and non-members) access to network services at the same time. As before, authorized MUs are provided extensive access to network services while non-authorized MUs are only allowed access to public domain network services.

While certain exemplary embodiments have been described and shown in the accompanying drawings, it is to be understood that such embodiments are merely illustrative of and not restrictive on the broad invention, and that this invention not be limited to the specific constructions and arrangements shown and described, since various other modifications are possible. For instance, while the invention has been described in the context of the IEEE 802.11 standard, it may also be implemented with other communication standards, such as Hyperlan I and Hyperlan II (specified by the European Telecommunications Standardization Institute). Additionally, it is possible to implement the invention or some of its features in hardware, programmable devices, firmware, software or a combination thereof. For instance, all or parts of the methods described herein may be performed by a processor within an AP and/or MU. The invention or parts of the invention may also be embodied in a processor-readable storage medium or machine-readable medium such as a magnetic, optical, or semiconductor storage medium.